(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/24435 A1

(51) International Patent Classification[7]: H04L 9/00, 9/08

(21) International Application Number: PCT/NL00/00688

(22) International Filing Date:
26 September 2000 (26.09.2000)

(25) Filing Language: Dutch

(26) Publication Language: English

(30) Priority Data:
1013148 28 September 1999 (28.09.1999) NL

(71) Applicant *(for all designated States except US)*: **3TP-INTERNATIONAL B.V.** [NL/NL]; Dorpsstraat 1, NL-5260 AE Vught (NL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **VAN RIJN, Dominicus, Henricus, Marie** [NL/NL]; Heunpark 1711, NL-5261 WB Vught (NL).

(74) Agent: **VAN DEN HEUVEL, Henricus, Theodorus**; Octrooibureau LIOC, P.O. Box 1514, NL-5200 BN s-Hertogenbosch (NL).

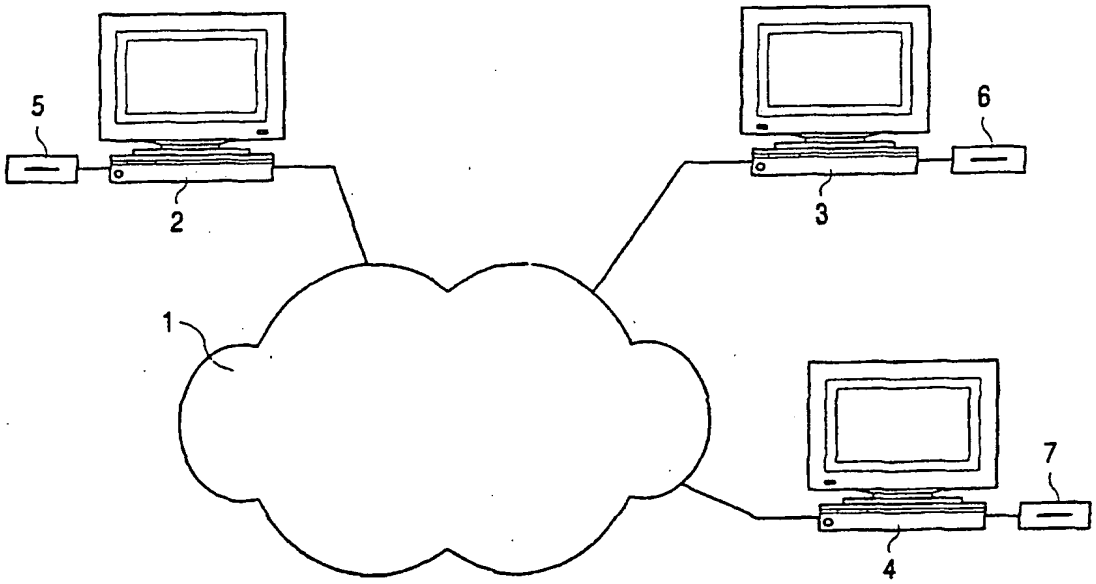
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: METHOD FOR SECURING DATA, KEY AND COMMUNICATION NETWORK FOR APPLYING THE METHOD



(57) Abstract: The invention relates to a method for securing data by encrypted transmission of the data, wherein at least one data transmitter and at least one data receiver are both provided with physically embodied keys for coding respectively decoding transmitted data such that a key code sent together with the transmitted data is unnecessary. The invention also relates to a method for securing data by encoded storage of the data, wherein prior to storage the data is coded with a physically embodied key and upon retrieval is decoded with a physically embodied key. The invention further provides a key and a communication network for applying in these methods.

WO 01/24435 A1

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for securing data, key and communication network for applying the method

The invention relates to a method for securing data by encoded transmission and/or storage of the data. The invention also relates to a key and a communication network for performing such a method.

The increase in electronic data storage and electronic data exchange also entails an increased need to secure this data. Particularly the storage and exchange of data in larger networks, such as for instance Internet and Extranet, results in much use being made of coding (encryption). The data for coding is processed for this purpose by an encryption program which adds a determined key code to the coded data. Decoding of the coded data is for instance possible using the same encryption program remotely from the location where the coding took place. The conversion program is controlled for this purpose by the key code. The drawback of the available methods is that the key code is added to the coded data so that this code is relatively simple to intercept. The key code can then be broken. Any key code can ultimately be broken, with a greater or lesser degree of effort. Particularly in the case of storage and exchange of confidential data (such as for instance financial transactions, privacy-related information, strategic information etc.) it is of great importance that this data be coded as securely as possible.

The present invention has for its object to provide an improved method for securing data, and a key and communication networks adapted to apply the method according to the invention.

The invention provides for this purpose a method for securing data by encrypted transmission of the data, wherein at least one data transmitter and at least one data receiver are both provided with physically embodied keys for coding respectively decoding transmitted data such that a key code sent together with the transmitted data is unnecessary. A combination of transmitter and receiver preferably makes use herein of a predetermined unique key code, and in preference these co-acting keys can further both be applied for coding and decoding. Not adding the key code to the coded data makes it practically impossible to undo the encryption. Only if possession of the key code is obtained can it possibly be broken, depending on the quality of the key code used. The

key codes are however physically embedded and held by the transmitter and receiver. The key code can therefore not be acquired from a network by electronic means. This results in a dramatic increase in the security of coded data. It is noted that the method can only be applied when both transmitter and receiver possess a physically embodied key, wherein these keys must also be mutually compatible. When transmitter and receiver make use of a determined unique key code, no outsider at all will be able to decode the data traffic between these parties. When both co-acting keys are employed for both coding and decoding it is possible for two parties to be able to communicate fully with each other at an unprecedentedly high level of security.

In another preferred application of the method a user group of a plurality of participants makes use of a plurality of keys for mutual communication such that each combination of two participants in the user group applies a unique mutual key code. A cluster of users therefore who can all communicate with each other without other participants in the group being able to decode the data traffic between a transmitter and receiver in the group. The user group can additionally be provided with one or more collective key codes, thereby enabling direct communication with sub-groups or the whole user group. Communication of groups of users is thus also secured.

In the case of for instance loss of a key or when for other reasons a user must be excluded from further secured data exchange, a key can be remotely deactivated once the signal therefor has been given at a central position. One condition for deactivation is that the key to be deactivated is then employed to decode respectively code data, since only when the central disabling signal reaches the card will it be disabled. The deactivation of a key is preferably irreversible, so that a thus deactivated key is not restorable and cannot be employed for later, possibly fraudulent use.

The invention also provides a method for securing data by encoded storage of the data, wherein prior to storage the data is coded with a physically embodied key and upon retrieval is decoded with a physically embodied key. In accordance with the method for securing the data to be transmitted according to the invention, the key code does not form part of the coded data, in this case when it is stored. If an unauthorized person

comes into possession of the coded data, there is absolutely no possibility of decoding this data, because of the unprecedentedly high level of security due to the absence of the key code.

In a preferred application of this method a plurality of physically embodied keys are provided with a corresponding key code for decoding the stored data. A plurality of key holders can thus decode stored coded data. A plurality of users can thus acquire access in a secure manner to protected information. When a plurality of physically embodied keys are provided with a corresponding key code for coding of data prior to storage, multiple users can also store coded data.

In a preferred application of the method a key is remotely deactivated once the signal therefor is given at a central position and the key to be deactivated is employed to decode respectively code data. In accordance with the above description relating to deactivation of a key; it may be desired to disable a key in a particular situation. An initiative must be taken at a central position to bring this about. When the key for disabling then comes into contact, either directly or indirectly, with the central position where the signal for disabling has been given, the key will be disabled. The moment of disabling is therefore generally the first time the key is used after the disabling signal has been given.

The invention moreover provides a method for coding respectively decoding data, wherein prior to conversion the data for processing is accessed by at least two physically embodied sub-keys. It is herein possible for the data for processing to be simultaneously accessed by at least two physically embodied keys, but it is also possible to apply the method such that the data for processing must be accessed by at least two physically embodied sub-keys within a predetermined period of time. These keys also have key codes which are not added to the coded data. This method enables decoding of coded data only when at least two key codes are entered, optionally within a determined space of time.

The invention further provides a key for performing the above described method, wherein the key comprises an electronic component, such as for instance a chip, in which an electronic key code is embedded. In a preferred embodiment the electronic component is incorporated in a card, which card is also provided with contact surfaces connected to the electronic component. Such a key can contain very complex algorithms with for instance time-dependent keys. It is also possible to embody such keys such that they contain paired key codes which only co-act with the key code of one other key. This pairing can already be arranged during manufacture. Clusters of users for instance, also referred to above as user groups, can thus also be incorporated in the electronic component at a production stage. Here can be envisaged for instance a user group of a hundred individuals, each using unique mutual key codes. The use of a card, for instance with the size of a credit card, is user-friendly since cards of such a format are generally used, so that the management of such a card is also a normal phenomenon. Particularly advantageous is the use of a so-called "smartcard" which is provided externally with electronic contact surfaces for connection of the electronic component to read means.

The invention further provides a communication network for transmitting and/or storing data provided with at least one key reader for reading an above described key such that one of the above described methods can be applied. The communication network requires only a limited modification; the network must be provided with key readers, for instance smartcard readers, at the positions where transmitters and/or receivers are connected.

The present invention will be further elucidated with reference to the non-limitative embodiments shown in the following figures. Herein:

Figure 1 shows a schematic view of a communication network according to the invention,

Figure 2 shows a view of a key card according to the invention, and

Figure 3 shows a view of a very limited communication network according to the invention.

Figure 1 shows a schematically depicted network 1 to which are connected three work-stations 2, 3, 4. Each of the work-stations 2, 3, 4 is provided respectively with its own key reader 5, 6, 7. Coded data exchange between work-stations 2 and 3 is only possible when two keys, for instance cards which are programmed/adjusted to a common key code, are inserted into key readers 5, 6. The coded data on network 1 contains no key code part and cannot therefore be decoded, or hardly so, by unauthorized persons. For communication between work-station 3 and work-station 4 the same keys can be used as for communication between work-stations 2 and 3. It is however also possible for two other key holders to make use of these work-stations or for one of the above mentioned key holders to now communicate with a new key holder. The earlier used key must contain for this purpose a specific other key code which is adjusted to the key code of the new user. Instead of mutual communication between two parties it is also possible to provide multiple users with the same key code so that it is possible to communicate in groups.

As stated, the keys must preferably be adjusted to mutual communication during production. The cards will therefore have to be marketed as sets or larger groups. Another, slightly less secure option is to make the cards mutually compatible after the production stage, for instance by means of reciprocal input of the same setup code, which is translated by the key to a key code.

Figure 2 shows a card 8 provided with standardized electronic contact surfaces 9. Such a card 8 is also referred to as a smartcard. An electronic chip (not shown) containing the key code is situated in card 8.

Figure 3 shows a very limited network 10 consisting of a work-station 11 to which are connected two key readers 12, 13. Work-station 11 can for instance be used for coded data storage, this data only being decodable when two keys co-acting for this purpose are inserted into key readers 12, 13.

When two co-acting cards 8 are made commercially available which are both adapted to code and decode data, it may be useful to add to the set an additional card 8 with which

it is only possible to decode. If one of the two fully functioning cards 8 is lost, the card suitable only for decoding can then be employed for a time until a complete new set has been ordered. The spare card 8, which is adapted only to decode, must of course be kept in a secure location. If one of the two fully functioning cards 8 is lost, this card can be made unusable in accordance with the foregoing description.

Although the invention is described with reference to only a few embodiments, it will be apparent to all that the invention is by no means limited to the described and shown embodiments. On the contrary, many variations are still possible for a skilled person within the scope of the invention.

Claims

1. Method for securing data by encrypted transmission of the data, wherein at least one data transmitter and at least one data receiver are both provided with physically embodied keys for coding respectively decoding transmitted data such that a key code sent together with the transmitted data is unnecessary.

2. Method as claimed in claim 1, wherein a combination of transmitter and receiver makes use of a predetermined unique key code.

3. Method as claimed in claim 1 or 2, wherein the co-acting keys are both applied for coding and decoding.

4. Method as claimed in any of the foregoing claims, wherein a user group of a plurality of participants makes use of a plurality of keys for mutual communication such that each combination of two participants in the user group applies a unique mutual key code.

5. Method as claimed in any of the foregoing claims, wherein a key is remotely deactivated once the signal therefor has been given at a central position and the key to be deactivated is then employed to decode respectively code data.

6. Method for securing data by encoded storage of the data, wherein prior to storage the data is coded with a physically embodied key and upon retrieval is decoded with a physically embodied key.

7. Method as claimed in claim 6, wherein a plurality of physically embodied keys are provided with a corresponding key code for decoding the stored data.

8. Method as claimed in claim 6 or 7, wherein a plurality of physically embodied keys are provided with a corresponding key code for coding of data prior to storage.

9. Method as claimed in any of the claims 6-8, wherein a key is remotely deactivated once the signal therefor is given at a central position and the key to be deactivated is employed to decode respectively code data.

10. Method for coding respectively decoding data, wherein prior to conversion the data for processing is accessed by at least two physically embodied sub-keys.

11. Method as claimed in claim 10, wherein the data for processing is simultaneously accessed by at least two physically embodied sub-keys.

12. Method as claimed in claim 10, wherein the data for processing is accessed by at least two physically embodied sub-keys within a predetermined period of time.

13. Key for performing a method as claimed in any of the claims 1-12, wherein the key comprises an electronic component, such as for instance a chip, in which an electronic key code is embedded.

14. Key as claimed in claim 13, wherein the electronic component is incorporated in a card, which card is also provided with contact surfaces connected to the electronic component.

15. Communication network for transmitting and/or storing data provided with at least one key reader for reading a key as claimed in claim 13 or 14 such that a method as claimed in any of the claims 1-12 can be applied.

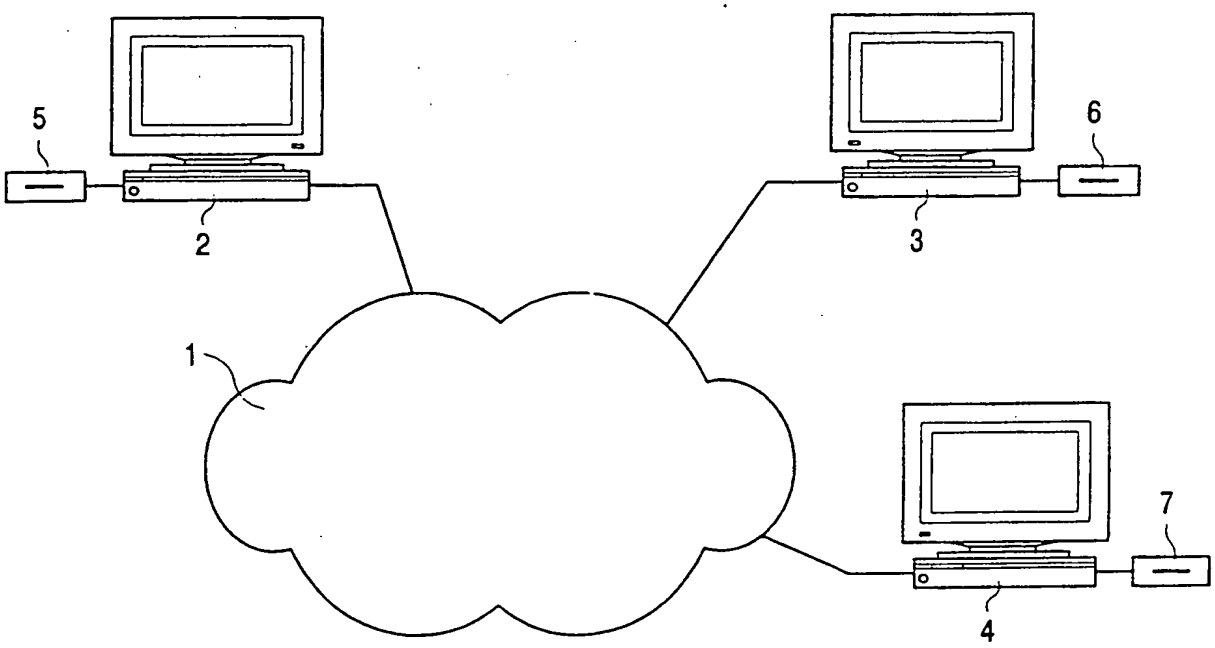


FIG. 1

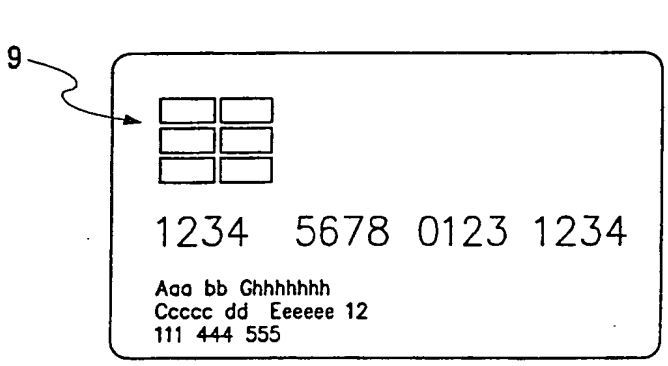


FIG. 2

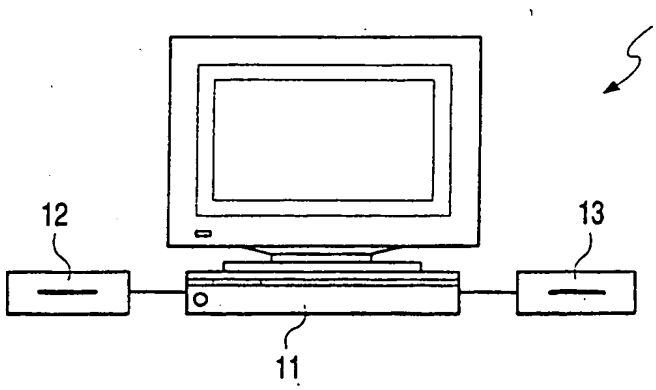


FIG. 3

INTERNATIONAL SEARCH REPORT

Intern. al Application No
PCT/NL 00/00688

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/00 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 613 105 A (FRANCE TELECOM) 31 August 1994 (1994-08-31) column 3, line 38 - line 44 column 4, line 4 -column 5, line 42	1,4,10, 11,13
X	WO 98 39745 A (DEUTSCHE TELEKOM AG) 11 September 1998 (1998-09-11) abstract	6
A	page 2, line 23 -page 3, line 18	5,9

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2001	29/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/NL 00/00688

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FERREIRA R C: "THE SMART CARD: A HIGH SECURITY TOOL IN EDP" PHILIPS TELECOMMUNICATION REVIEW,NL,PHILIPS TELECOMMUNICATIE INDUSTRIE N.V. HILVERSUM, vol. 47, no. 3, 1 September 1989 (1989-09-01), pages 1-19, XP000072642 page 3, last paragraph -page 5, line 22 ---	1,6
X	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 13, 30 November 1998 (1998-11-30) & JP 10 214233 A (TOSHIBA CORP), 11 August 1998 (1998-08-11) abstract -----	6

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna al Application No
PCT/NL 00/00688

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0613105 A	31-08-1994	FR 2702066 A	02-09-1994
		DE 69408176 D	05-03-1998
		DE 69408176 T	30-07-1998
		US 5602915 A	11-02-1997
WO 9839745 A	11-09-1998	EP 0970449 A	12-01-2000
		NO 994235 A	28-10-1999
JP 10214233 A	11-08-1998	US 6085323 A	04-07-2000

Form PCT/ISA/210 (patent family annex) (July 1992)